UNITED STATES DISTRICT COURT

for the
District of South Dakota

In the Matter of the Search of:
The property located at [redacted]

Case No. 5:20-mj-20

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the District of South Dakota *(identify the person or describe the property to be searched and give its location)*:

See **ATTACHMENT A**, attached hereto and incorporated by reference

I find that the affidavit, or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

Evidence of a crime in violation of 18 U.S.C. §§ 2252 & 2252A as described in **ATTACHMENT B**, attached hereto and incorporated by reference.

I find that the affidavit, or any recorded testimony, establishes probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before Feb. 12, 2020 *(not to exceed 14 days)*

☑ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Daneta Wollmann.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for _____ days *(not to exceed 30)*. ☐ until, the facts justifying, the later specific date of _____.

☐ I find that good cause has been established to authorize the officer executing this warrant to not provide notice prior to the execution of the search warrant, i.e., "no knock".

Date and time issued: 1-29-2020 10:15am

Judge's signature

City and state: Rapid City, SD

Daneta Wollmann, U.S. Magistrate

cc: AUSA Collins + Agent

Return

Case No.: 5:20-mj-20	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date:

Executing officer's signature

Printed name and title

UNITED STATES DISTRICT COURT

for the
District of South Dakota

IN THE MATTER OF THE SEARCH OF the property located at [redacted]

Case No. 5:20-mj-20

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SEE "ATTACHMENT A", which is attached to and incorporated in this Application and Affidavit

located in the District of South Dakota, there is now concealed *(identify the person or describe the property to be seized)*:

SEE "ATTACHMENT B", which is attached to and incorporated in this Application and Affidavit

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 2252 & 2252A	Receipt and possession of child pornography

The application is based on these facts:

☒ Continued on the attached affidavit, which is incorporated by reference.

☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

☐ Your applicant requests that no notice be given prior to the execution of the search warrant, i.e., "no knock", the basis of which is set forth in the attached affidavit.

☐ Your applicant requests authorization to serve the search warrant any time day or night pursuant to Fed. R. Crim. P. 41(e)(2)(A)(ii), the basis of which is set forth in the attached affidavit.

Special Agent Michelle Pohlen

Sworn to before me and:
☑ signed in my presence.
☐ submitted, attested to, and acknowledged by reliable electronic means.

Date: 1-29-2020

Judge's signature

City and state: Rapid City, SD

Daneta Wollmann, U.S. Magistrate
Printed name and title

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
WESTERN DIVISION

IN THE MATTER OF THE SEARCH OF:
The property located at [redacted]

CASE NUMBER: 5:20-mj-20

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT APPLICATION

SEALED

State of South Dakota)
) ss
County of Pennington)

I, Michelle Pohlen, Special Agent with Homeland Security Investigations (HSI), and currently assigned to the Rapid City, South Dakota Resident Agent in Charge (RAC) Office, being duly sworn, states as follows:

1. I have been a Special Agent (SA) with HSI since March 2019. In September 2019, I completed the Homeland Security Investigations Special Agent Training (HSISAT) at the Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia. In June 2019, I completed the Criminal Investigator Training Program (CITP), also located at FLETC in Glynco, GA. Prior to becoming a Special Agent, I was employed as a Federal Air Marshal with the Federal Air Marshal Service (FAMS) for two and a half years. Prior to FAMS, I served as a Police Officer with the Savannah Chatham Metropolitan Police Department (SCMPD) in Savannah, Georgia for one and a half years. I received a Bachelor of Arts degree in Law Enforcement in 2014.

2. During my law enforcement career, I have been involved in the investigation of cases involving the possession, receipt, and distribution of child pornography in violation of 18 U.S.C. §§ 2251, 2252, and 2252A. I have become familiar with the *modus operandi* of persons involved in the illegal production, distribution and possession of child pornography. Based on my experience and training, I am knowledgeable of the various means utilized by individuals who illegally produce, distribute, receive and possess child pornography.

3. I am aware that 18 U.S.C. §§ 2251, 2252 and 2252A, prohibit the production, distribution, receipt and possession of visual depictions of a minor engaging in sexually explicit conduct, using any means or facility of interstate or foreign commerce, including by computer or utilizing the internet.

4. The facts set forth in this affidavit are based on my personal knowledge; knowledge obtained from other individuals, including other law enforcement officers; interviews of persons with knowledge; my review of documents, interview reports and computer records related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience. This affidavit contains information necessary to support probable cause for this application and does not contain every material fact that I have learned during the course of this investigation; however, no information known to me that would tend to negate probable cause has been withheld from this affidavit.

ITEMS TO BE SEARCHED FOR AND SEIZED:

5. This affidavit is submitted in support of an application for a search warrant for the property located at [redacted] (hereinafter also referred to as SUBJECT PREMISES and photographically depicted in Attachments C and D). Additionally, your affiant seeks the warrant to authorize the search of any vehicles, outbuildings, or detached garages and the curtilage on the property; any persons on the property; and the content of any computer and electronic storage devices, cellular phones, tablets, and any other electronic storage devices, including but not limited to external and internal hard drives, thumb drives, flash drives, gaming devices with storage capability, storage discs, SD cards, cameras, cellular phones, smart phones and phones with photo-taking and/or internet access capabilities. I respectfully request the Court permit law enforcement to seize all such electronic devices located on the premises and further, to access and search the contents of said electronic devices without seeking an additional or separate warrant.

6. The warrant is being obtained in order to search for contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2251, 2252

and 2252A, which criminalize the production, distribution, receipt and possession of child pornography.

DEFINITIONS

7. The following definitions apply to this Affidavit and Attachments A and B:

a. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. "Child Erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

c. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. "Cloud-based storage service," as used herein, refers to a publically accessible, online storage provider that collectors of child pornography can use to store and trade child pornography in larger volumes. Users of such a service can share links and associated passwords to their stored files with other traders of child pornography in order to grant access to their collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop and laptop computers, mobile phones, and tablets, anywhere and at any time. An individual with the password to file stored on a cloud-based service does not need to be a user of the service to access the file. Access is free and readily available to anyone who has an internet connection.

e. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, and mobile phones and devices. See 18 U.S.C. § 1030(e)(1).

f. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units,

internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

g. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

h. "Computer-related documentation," as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

i. "Computer passwords, pass-phrases and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass-phrase (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips,

and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

j. A provider of "Electronic Communication Service" ("ESP"), as defined in 18 U.S.C. § 2510(15), is any service that provides to users thereof the ability to send or receive wire or electronic communications. For example, "telephone companies and electronic mail companies" generally act as providers of electronic communication services. *See* S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3568.

k. "Electronic Storage Device" includes but is not limited to external and internal hard drives, thumb drives, flash drives, SD cards, gaming devices with storage capability, storage discs (CDs and DVDs), cameras, cellular phones, smart phones and phones with photo-taking and/or internet access capabilities, and any "cloud" storage by any provider.

l. "File Transfer Protocol" ("FTP"), as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.

m. "Hash value," as used herein, refers to a unique alpha-numeric identifier for a digital file. A hash value is generated by a mathematical algorithm, based on the file's content. A hash value is a file's "digital fingerprint." Two files having identical content will have the same hash value, even if the file names are different. On the other hand, any change to the data in a file, however slight, will change the file's hash value, even if the file name is unchanged. Thus, if two files have the same hash value, they are said to be identical, even if they have different file names.

n. "Internet Protocol address" or "IP address," as used herein, refers to a unique number used by a computer or other digital device to access the Internet. An IP address is one of two versions. Internet Protocol Version 4 (IPV4) or Internet Protocol Version 6 (IPV6). IPV4 looks like a series of four numbers, each in the range 1-255, separated by periods. IPV6 looks like a series of 8 numbers or letters separated by a colon. Each series of numbers will be 0-9 and/or a-f. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be properly directed from its source to its destination. Most Internet Service Providers (ISPs – defined below) control a range of OP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a

particular IP address that is used each time the computer accesses the Internet. ISPs

o. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

p. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

q. "Remote Computing Service" ("RCS"), as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

r. "Short Message Service" ("SMS"), as used herein, is a service used to send text messages to mobile phones. SMS is also often referred to as texting, sending text messages or text messaging. The service allows for short text messages to be sent from one cell phone to another cell phone or from the Web to another cell phone. The term "computer," as defined in 18 U.S.C. § 1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage

facility or communications facility directly related to or operating in conjunction with such device.

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, THE INTERNET, AND EMAIL

8. I have training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras and smartphones with cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera or smartphone to the computer. In the last ten years, the resolution of pictures taken by digital cameras and smartphones has increased dramatically, meaning that such pictures have become sharper and crisper. Photos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards often store up to 32 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video

footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTPs) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-Terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and

"thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them). Media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer or external media in most cases.

g. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these

purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

9. Based upon my training and experience, as well as information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices including hard disk drives, floppy disks, compact disks, magnetic tapes and memory chips. I also know that during a search of physical premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In

addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also

attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband or instrumentalities of a crime.

10. Based on my training and experience, as well as my consultation with other agents who have been involved in computer searches, searching computerized information for evidence or instrumentalities of a crime often requires the seizure of all of a computer system's input and output peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. There are several reasons that compel this conclusion:

a. The peripheral devices that allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above.

In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices; and

b. In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices, as well as the central processing unit (CPU). In cases like the instant one where the evidence consists partly of image files, the monitor and printer are also essential to show the nature and quality of the graphic images which the system could produce. Further, the analyst again needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval.

11. Additionally, based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of so-called "wireless routers," which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be "secured" (in that they require an individual to enter an alphanumeric key or password

before gaining access to the network) or "unsecured" (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

PROBABLE CAUSE AND BACKGROUND OF THE INVESTIGATION

12. On January 2, 2020, Detective Elliott Harding received four cybertips from the National Center from Missing and Exploited Children (NCMEC): 59190015, 59738685, 59844348 and 60115237.

CYBERTIP 59190015:

13. The images in cybertip 59190015 were locked so Harding obtained a search warrant to unlock the files from the 7th Judicial Circuit, South Dakota. He learned the following:

Incident Information:
Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 11-12-2019 01:13:40 UTC.
Description of Incident Time: The incident date refers to the approximate date and time Google became aware of the reported material.
Suspect Name: Jay
Date of Birth: 08-27-2000

Email Address: dogeye17@gmail.com (Verified)
Email Address: jm970684@gmail.com

Additional Information Submitted by the Reporting ESP:
Google became aware of the reported content which was stored in Google Drive infrastructure
Uploaded File Information: Number of uploaded files: 72

14. Det. Harding investigated the IP addresses associated with cybertip 59190015 and learned the following: 209.159.232.149: Vast Broadband; 45.33.129.40: CloudMosa; 107.178.38.28: CloudMosa; 109.169.63.48: Iomart Hosting Limited.

15. Per Harding: Within this portion of the CyberTip, it provided many Login IP addresses from 2/10/19 and 11/4/19. Many of the IP addresses listed were 209.159.232.149. There were single instances of IP addresses 45.33.129.40, 104.244.78.233 and 107.178.38.28. There were two instances of 109.169.63.48.

16. Det. Harding observed the images associated with cybertip 59190015. He observed a total of 71 files constituting child pornography. The images included a video of a 7-10 year old girl being anally raped; a picture of a 4-6 year old girl inserting her finger into another girl, of similar age's vagina while a male ejaculated into one of the girl's mouth; a picture of a 4-5 year old girl with an unknown object inserted in her vagina and anus; a video of a 3-5 year old girl digitally manipulating an adult penis; a video of a 2-4 year old being manipulated so her finger went in and out of her vagina; a video of a man inserting an unknown object into the vagina of a 6-8 year old; and a video of one 3-5 year old licking another like-aged female's anus and buttocks.

CYBERTIP 59738685:

17. NCMEC provided the following information regarding cybertip 59738685:

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)

Incident Time: 11-20-2019 08:00:59 UTC

Description of Incident Time: The incident date refers to the approximate date and time Google became aware of the reported material.

Suspect
The information under the Suspect heading was the same as CyberTip 59190015 mentioned above.

Additional Information Submitted by the Reporting ESP
Google became aware of the reported content which was stored in Google Drive infrastructure

Uploaded File Information
Number of uploaded files: 4

18. Det. Harding observed four images of child pornography related to this cybertip. The images included a picture of a 6-9 year old with her genitals partially exposed; a video of a 6-9 year old girl exposing her vagina; a picture of a 2-4 year old girl squatting and exposing her vagina with a sucker in her mouth; and a picture of a 6-8 year old girl exposing her vagina and breasts.

CYBERTIP 60115237:

19. Det. Harding learned that in cybertip 60115237, Google reported Anime/Drawing/Virtual Child Pornography to NCMEC: **Incident Information Incident Type: Child Pornography (possession, manufacture, and distribution)**

Incident Time: 11-26-2019 03:41:35 UTC
Description of Incident Time: The incident date refers to the approximate date and time Google became aware of the reported material.

Suspect: The information under the Suspect heading was the same as CyberTip 59190015 and 59738685 mentioned above.

Additional Information Submitted by the Reporting ESP: Google became aware of the reported content which was stored in Google Drive infrastructure
Uploaded File Information: Number of uploaded files: 1

20. There was one file contained in this cybertip and it was a video of animated child pornography of a 5-7 year old girl in various states of nudity and engaging in masturbation with playground equipment and also engaging in sexual intercourse with a like-age male.

CYBERTIP 59844348

21. Detective Harding received a fourth cybertip related to the same user as the three described above. The following is the information he received from NCMEC:

Incident Information
Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 11-22-2019 03:11:39 UTC
Description of Incident Time: The incident date refers to the approximate date and time Google became aware of the reported material.

Suspect: The information under the Suspect heading was the same as CyberTips 59190015, 59738685 and 60115237 mentioned above.

Additional Information Submitted by the Reporting ESP: Google became aware of the reported content which was stored in Google Drive infrastructure

Uploaded File Information: Number of uploaded files: 1

22. Det. Harding reviewed the image associated with this cybertip. He described it as a photo of an 8-11 year old girl, standing on a couch with her genitals and breasts exposed.

23. On January 9, 2020, Det. Harding sent a request to HSI Analyst Amber Cooper asking her to identify the suspect based on the information provided in the four CyberTips mentioned above. Analyst Cooper subpoenaed Vast Broadband regarding the IP address 209.159.232.149 which made up the majority of the suspect login IP addresses. Vast returned the following information:

Rebecca Miller
[redacted]

24. Analyst Cooper reviewed obituary information published online provided the following associated family member names:

[redacted]

25. Analyst Cooper conducted a driver's license inquiry which showed James Miller (DOB [redacted]) lived at [redacted] (the SUBJECT PREMISES).

26. She also ran a criminal history inquiry, which provided that James Miller had been arrested for solicitation of a minor and the case is currently pending. Det. Harding reviewed the police reports related to that offense which confirmed that Miller lives at the SUBJECT PREMISES. The allegations were that in the summer of 2018, Miller separately approached three girls, one 11 years old and two 12 years old, playing around his apartment complex and asked

to take pictures of them. One of the girls indicated that Miller asked to take pictures of her breasts and vagina.

27. Officers investigating the solicitation matter interviewed Rebecca Miller and James Miller at the SUBJECT PREMISES. Rebecca invited the officers into the apartment and retrieved James from a bedroom. Upon being asked if he was willing to participate in an interview, James indicated that he would first have to pause his computer game and returned to the room. James denied asking the girls for pictures. Rebecca indicated that despite James being an adult, she had guardianship of James because he is autistic and cannot make decisions for himself.

28. All four of the cybertips were associated with the same email accounts, which were dogeye17@gmail.com and jm970684@gmail.com. Analyst Cooper issued subpoenas to Google to get user information regarding dogeye17@gmail.com. Google responded that email's recovery email was the jm970684@gmail.com account and the user's name was "James Miller".

29. On January 27, 2020, Det. Harding went to the SUBJECT PREMISES and verified that the Millers appear to still live there and Det. Jeremy Stauffacher photographed the location.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO HAVE A SEXUAL INTEREST IN CHILDREN AND/OR WHO PRODUCE, RECEIVE AND/OR POSSESS CHILD PORNOGRAPHY

30. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain

characteristics common to individuals who have a sexual interest in children and/or receive, or possess images of child pornography:

a. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography almost always possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy

and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children often retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals who have a sexual interest in children and/or receive, or possess images of child pornography often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly.

e. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography prefer not to be without

their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Thus, even if James Miller uses a portable device (such as a mobile cell phone) to access the internet and child pornography, it is more likely than not that evidence of this access will be found in his home, the SUBJECT PREMISES, as well as on electronic devices found in the home, as previously detailed and as set forth in Attachment A.

REQUEST FOR SEALING OF APPLICATION/AFFIDAVIT

31. I request that the Court order that all papers submitted in support of this application, including this affidavit, the application, the warrant, and the Order itself, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give the target an opportunity to flee, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

CONCLUSION

32. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that there exists evidence of a crime, contraband, instrumentalities, and/or fruits of violations of criminal laws as specified herein, are located at the SUBJECT PREMISES, described further in Attachment A. I respectfully request that this Court issue a search warrant for

the SUBJECT PREMISES, authorizing the seizure and search of the items described in Attachment B.

33. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

Special Agent Michelle Pohlen
Department of Homeland Security
Investigations

SUBSCRIBED and SWORN to

dw in my presence
____ by reliable electronic means

this 29th day of January, 2020.

DANETA WOLLMANN
U.S. MAGISTRATE JUDGE

ATTACHMENT A
Property to Be Searched

- The property located at [redacted] (also referred to in this affidavit as SUBJECT PREMISES and photographically depicted in Attachments C and D);
- any vehicles associated with [redacted];
- outbuildings or detached garages and the curtilage on the property associated with [redacted]
- and any persons on the property associated with [redacted];
- the content of any seized computer and electronic storage devices, cellular phones, tablets, and any other electronic storage devices, including but not limited to external and internal hard drives, thumb drives, flash drives, gaming devices with storage capability, storage discs, SD cards, cameras, cellular phones, smart phones and phones with photo-taking and/or internet access capabilities.

ATTACHMENT B

ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2251, 2252 and 2252A:

1. Computers, cell phones or storage media used as a means to commit the violations described above.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
    a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
    b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user

entered into any Internet search engine, and records of user-typed web addresses; and

m. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.

4. Child pornography and child erotica.

5. Records, information, and items relating to violations of the statutes described above including:

   a. Records, information, and items relating to the occupancy or ownership of [redacted], including utility and telephone bills, mail envelopes, or addressed correspondence; Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;

   b. Records and information relating to the identity or location of the persons suspected of violating the statutes described above; and

   c. Records and information relating to sexual exploitation of children, including correspondence and communications between various Seller and Buyer Accounts.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such

as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies, CDs, DVDs).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which records computer data. Examples include external and internal hard drives, thumb drives, flash drives, gaming devices with storage capability, storage discs, SD cards, hard disks, RAM, flash memory, CDs, DVDs, and other magnetic or optical media.

ATTACHMENT C

ATTACHMENT D